Quality Assurance Surveillance Plan (QASP)

Title: Priority Telecommunications Services (PTS)

1.0 Background

The National Security and Emergency Preparedness (NS/EP) PTS program responds to White House tasking to address the communications for Continuity of Operations (COOP) and Continuity of Government (COG). Through NS/EP enhancements to the national telecommunications infrastructure, the ECD can effectively and economically address the COOP/COG needs while providing a significant benefit of assured communications during NS/EP incidents to the broader national, state, local and non-government NS/EP community. NS/EP PTS, by leveraging the Public Switched Network (PSN), help to ensure the preparedness of the Nation, to prevent, respond to, and recover from, threatened and actual terrorist attacks, major disasters and other emergencies in accordance with the National response framework, National infrastructure protection plan, and is supportive of the National Incident Management System. NS/EP PTS has, and will continue to support NS/EP users' telecommunications requirements during disasters and emergencies.

2.0 Purpose

The purpose of this QASP is to ensure that the Contractor meets the Key Performance Parameters stated in the Functional Requirements Specifications (FRS) and incorporated in Performance Work Statement (PWS). The QASP provides the Emergency Communications Division (ECD) the ability to conduct surveillance activities of Contractor performance during the life of the contract. The QASP details how the ECD will monitor, evaluate, and document Contractor performance for PTS.

3.0 QASP Work Requirements

In response to the PTS PWS, the Contractor shall prepare a QASP for assessing performance to ensure compliance with the Government's KPPs described below. . The QASP shall describe the surveillance schedule, surveillance methods, performance measures/metrics, and non-monetary incentives (if applicable). As part of the QASP, the Contractor shall prepare a Performance Requirements Summary (PRS) matrix (Attachment 8) to address all requirements of the SOO. The Contractor shall include in the matrix all changes and additions being proposed.

NGN PS Key Performance Parameters (KPP)

Performance Metrics	Performance Objectives	
Metric	**Threshold**	**Objective**
Wireless Call Completion Rate	≥ 0.80	≥ 0.90
Wireline Call Completion Rate	≥ 0.90	≥ 0.95
Wireless Call Quality (Mean Opinion Score)	≥ 3.0 for ≥ 0.90 answered calls	≥ 3.5 for ≥ 0.95 answered calls
Wireline Call Quality (Mean Opinion Score)	≥ 3.5 for ≥ 0.90 answered calls	≥ 4.0 for ≥ 0.95 answered calls
Service Availability	≥ 0.998	≥ 0.999
Expedited User Provisioning	90% of users within 48 hours	95% of users within 48 hours

NGN PS Key Performance Parameters (KPP) Technical Descriptions

KPP Description	KPP Details
Call Completion Rate is the percentage of priority call attempts that are completed (as defined below) for all valid, authorized attempts to valid destinations during the measurement period. This measure ensures that during national incidents and throughout periods of congestion caused by any of the range of threats and hazards identified in the CONOPS, the service is responsive to user requests for priority. Service providers supply periodic usage reports that include performance data and traffic characteristics. The service providers provide information on all priority calls routed through their networks. This includes counts of items including call attempts, calls blocked, and calls queued.	The formula is (calls completed)* 100 / (valid calls attempted, if any) where: • "**calls completed**" is the number of NGN priority call attempts during the measurement period that resulted in either a ringing tone, a user-busy tone, or an indication that the called party is not reachable or is out of service; • "**valid calls attempted**" is the number of NGN priority calls that were attempted with proper dialing during the measurement period to valid destination numbers by callers presenting valid authorization credentials.
Call Quality is a measure of voice intelligibility for priority service calls. Calls must have sufficient quality to be completely understandable by both parties. Mean Opinion Score and R-Factor are alternative measures of audio quality during a voice NGN priority call.	The R-Factor[40] can be produced by technology embedded in network equipment and end terminals; Mean Opinion Score can then be predicted by modeling and simulation or estimated from the R-Factor via the relationship. • Mean Opinion Score = 1 + (0.035) ∗ R + (.000007) ∗ R ∗ (R-60) ∗ (100-R). Mean Opinion Score, though traditionally devised as user-provided subjective values, can in fact be closely estimated from packet loss, jitter, and latency (delay) data obtained from network performance data or estimated through modeling and simulation.

Service Availability = (time that NGN PS are available) / (measurement time). The service is considered available when all service-specific systems are providing the functionality for which they were intended at the capacity for which the service was designed.	Service specific systems are network elements that are either dedicated exclusively to providing NGN PS related functionality (e.g., a dedicated authorization server), or are shared resources that provide service-related functionality as well as functionality specific to another, non-priority service. The NGN PS related functions include: • Priority services access authorization • Priority marking of signaling messages and media traffic for authorized calls • Priority processing of authorized calls
Expediter User Provisioning. The service request process can be expedited during emergencies to issue temporary emergency PIN cards, either as individual cards or as multi-use, shared-PIN organization cards. Expedited user provisioning is a measure of how quickly those requests are processed. This KPP measures the level of support provided to the user community.	

3.1 PTS Readiness Requirements.

FAR 37.102 establishes the policy to use the Performance Based Service Acquisition (PBSA) to the maximum extent practicable. For the PTS PWS, these requirements are defined in Attachment 6 (Performance Requirements Summary). These requirements must be supported by fully reliable provisioning processes that establish, manage, control and protect user capabilities and parameters that are stored in Contractor databases and deployed in the operational networks supporting PTS. The Contractor prepared QASP shall define the methods and products used to measure performance for PTS.

4.0 Primary Method of Surveillance

The Contractor prepared QASP shall define surveillance methods for all Government requirements to include the Contract Data Requirement List (CDRL) and proposed special reports. The Contractor shall provide specific details on the surveillance methods and techniques used with Readiness area of OAM&P.

5.0 Performance Standards

The Contractor prepared QASP submitted for Government approval shall define performance standards and metrics that reflect the level of service required by the Government to meet performance objectives.

6.0 Acceptable Quality Level

The Contractor prepared QASP shall contain recommendations on the AQL associated with requirements and performance standards. For readiness requirements under PBSA, the AQL is established at 100 percent to ensure the Government Emergency Telecommunications Service (GETS), GETS Voice over Internet Protocol (VoIP), Wireless Priority Service (WPS), and WPS Voice over Long Term Evolution (VoLTE) service parameters and provisioning are error free at all times. In the event the Contractor does not meet the established AQLs, the Contracting Officer has the right to exercise the disincentives stated in the QASP.

7.0 Evaluation Method

All products and processes will be evaluated after receipt of reporting deliverables or feedback on service operations. The readiness requirements shall be evaluated on the basis of recurring or periodical reporting as well as incident related or exception type reporting.

8.0 Disincentive

Disincentive: If any of the performance requirements does not meet the AQL set in the PRS table, when the performance is below the AQL standard, the Government will implement a disincentive withholding 25% of Award fees.

For the readiness requirements, the Contractor shall reimburse the Government 25% of the Award Fee if 100% AQL requirement is not met.

Maintaining the Master Database and Coordinate Changes with GETS and WPS Service Providers
The Contractor shall process all approved requests for GETS and WPS and coordinate these changes with the GETS and WPS service providers to ensure that only authorized subscribers have access to the service priority features. Automated processes and tools exist for these tasks.

Submitting Requests for GETS and WPS
Designated point of contact (POC) from organizations that have been approved to use GETS and WPS submit requests either through the GETS/WPS Information Delivery Service (G-WIDS) or through a preformatted spreadsheet. G-WIDS is a secure website that has been developed in cooperation with the Government. The Government Task Officer or designated official reviews these requests and mark acceptable entries as approved. The Contractor shall enter this data into the GETS and WPS Personal Identification Number (PIN) Subscriber Database.

G-WIDS
Organizational POCs and Alternate POCs have electronic access to the GETS card information needed to effectively execute their GETS and WPS administrative functions, including:

- Request GETS/WPS service for individuals in their organization
- Search and review GETS/WPS subscriber data
- Request changes for their existing GETS/WPS subscribers
- Request GETS/WPS POC database application data sets for download
- Track transaction requests
- Certify Call Detail Records (CDRs)
- Download listings of current GETS and WPS subscribers

- Download training documents, NewsNotes, and GETS/WPS User Council Meeting briefing slides and summaries.

POCs can only see records related to their accounts, with one exception: G-WIDS allow a hierarchy of POCs, so that larger organizations can decentralize management of their accounts while still allowing for oversight from a central POC. In addition, the site also allows authorized personnel to review all new requests and approve, cancel, disapprove or put them on hold.

GETS and WPS PIN Subscriber Database
The GETS and WPS PIN subscriber Database is the official repository for all active and deleted GETS and WPS service. This database is the source of all data transmitted to the GETS and WPS Carriers regarding which GETS card numbers or priority cellular devices are active. It records changes to those services and groups subscribers under their identified POCs. Subscriber records include the unique 12-digit GETS card number issued to each subscriber, their name, title, organization, phone numbers, email address, mailing address, and whether they have international and number translation calling privileges. The database also stores the Program Designator Code, which are the billing codes for non-federal organizations. A dedicated database administrator is responsible for all updates to the system, including new data fields and implementing rules related to how data is to be processed.

Though all data going into the database is unclassified, 25 percent or more of it, together in a single repository received a security classification of Secret. Because of this, the GETS/WPS PIN subscriber database resides in a secure facility, with access only through secure workstations.

Processing GETS/WPS Requests
After receiving approved request for GETS/WPS, the Contractor makes the appropriate updates in the GETS/WPS PIN Subscriber Database. Then it will electronically send the necessary information to the appropriate carriers to activate service in their networks. For GETS requests, staff will test the card, package it with instructions and send it to the requesting POC. For WPS requests, when confirmation of activation comes back from the carrier, the Contractor notifies the requesting POC and, where possible, the WPS subscriber. Where the carrier is unable to activate WPS, the Contractor notifies the POC of the problem.

Expediting GETS/WPS Requests
There are mechanisms in place to provision GETS/WPS requests faster than normal processing allows. When a request on G-WIDS is labeled as an “expedite,” the Contractor management will receive notifications every 30 minutes until it has been handled. For GETS requests, provisions are in place to either ship the card by FedEx or transmit the card number electronically. If necessary, it is possible to assign a GETS card number from and existing stockpile card that is already active. For WPS requests, it is still necessary to coordinate with the WPS carrier and notify the POC upon completion.

Providing Data Subsets
On a weekly basis sends a sanitized version of the data to the NCS NS/EP Priority Telecommunications Service Center (currently owned and operated by an operations support Contractor) for analysis and as a reference for staff reviewing new requests.

Ensuring the Synchronization of GETS and WPS Databases
Twice a year, the Contractor completes two synchronizations of the GETS dataset with each of the LECs. Where there are discrepancies, the Contractor works with the carrier to resolve them and then compares their databases again. A similar process occurs for WPS, though this resynchronization process is critical because it is possible for a WPS subscriber to cancel cellular service or transfer to a new carrier without advising the ECD. In this situation, the Contractor notes in the GETS/WPS PIN Subscriber Database that WPS is no longer active on that phone.

User Assistance
When GETS/WPS subscribers have questions or cannot complete their calls, they call the Contractor who handles these calls 24x7 and keeps record of them. In the case of general questions, the Contractor will provide the answers where possible, or direct the caller to the appropriate resource if necessary. In the case of not being able to complete calls, the Contractor will troubleshoot to determine the problem. Where it is a matter of training the subscriber, the Contractor will provide that instruction over the phone. If the problem appears to be specific to the caller's facility, the Contractor will work with that facility's telecommunications manager until the problem is resolved. Similarly, the Contractor will report LECs or wireless carrier problems to the appropriate resource within that carrier and track it until resolved. Where necessary the IC will escalate the question for assistance. The Contractor reports calls for user assistance on regular reports to the ECD.

Security Administration
The Contractor is responsible for ensuring that only authorized persons have access to GET/WPS data related to the Program Management Office, LECs, wireless carriers, or the Contractor itself. Three requirements drive processes related to supporting them. These requirements are: 1) all GETS card number information must be protected; 2) the Contractor must maintain a GETS number translation database; and 3) all carrier-provided call detail and performance data must be protected. This last requirement is a derived requirement. The processes supporting these requirements appear below.

GETS/WPS Database Maintenance
In order to protect GETS card number data, the Contractor uses standardized process to make any updates, regardless of the format in which the data was received. As mentioned above, the data received is unclassified, but 25 percent or more of the overall GETS/WPS PIN Subscriber Database is classified Secret. This forces restrictions on how the data is stored, handled, and who has access to it.

GETS PIN/Subscriber Database Swap-Out
Also supporting protection of GETS card number data, the Contractor can cancel all existing GETS card numbers and replace them within 24 hours of receiving notification

from the ECD. All GETS subscribers have a primary and alternate GETS card number. The alternate card numbers would have the same associated privileges as the primary number. In the event of compromise to the database, it is possible to substitute the alternate card number for the primary card number and forward these updates to each of the LECs. The Contractor would coordinate with ECD to determine the best way to distribute the new GETS cards numbers to respective POCS. There is no analogous process for WPS.

Carrier Data Protection

The Contractor is responsible for protecting call detail and other proprietary data from the LECs, and wireless carriers. Upon receipt of such information, the Contractor logs it and stores it in a secure facility. Because the aggregation of this data is considered classified, the hard disk storing it is used in an approved classified machine in a secured area. Outside regular business hours, the hard disk is stored in a GSA-approved safe.

Emergency Support

When the nature of an event requires extended and extensive monitoring and response, the ECD can formally request that the Contractor provide 24x7 staffing. The Contractor assigns teams representing the various functional areas required to respond to the event, and these teams' leaders have reach-back capability to the rest of the Contractor staff as needed. Until given directions to stand down, each shift leader reports back to the ECD with ongoing status updates and to receive further directions. Among the on-duty team's responsibilities is to make test calls into, and, if possible, out of, the affected area to determine GETS/WPS performance. Further, the Contractor reviews and analyzes the results of this and other data gathered from LECs, and wireless carriers at regular intervals and reports it back to the ECD. When the event is over, the Contractor provides a final report of GETS/WPS performance.